1. | | |
    |---|---|
    | Record Nr. | UNINA9910409666403321 |
    | Titolo | Advances in Cryptology – EUROCRYPT 2020 : 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II / / edited by Anne Canteaut, Yuval Ishai |
    | Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020 |
    | ISBN | 3-030-45724-9 |
    | Edizione | [1st ed. 2020.] |
    | Descrizione fisica | 1 online resource (xv, 861 pages) |
    | Collana | Security and Cryptology, , 2946-1863 ; ; 12106 |
    | Disciplina | 005.8
005.824 |
    | Soggetti | Cryptography
Data encryption (Computer science)
Database management
Computer networks
Data protection
Data structures (Computer science)
Information theory
Cryptology
Database Management System
Computer Communication Networks
Data and Information Security
Data Structures and Information Theory |
    | Lingua di pubblicazione | Inglese |
    | Formato | Materiale a stampa |
    | Livello bibliografico | Monografia |
    | Nota di contenuto | Generic Models -- Secure Computation I -- Quantum I -- Foundations -- Isogeny-Based Cryptography -- Lattice-Based Cryptography -- Symmetric Cryptography II -- Secure Computation II. |
    | Sommario/riassunto | The three volume-set LNCS 12105, 12106, and 12107 constitute the thoroughly refereed proceedings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2020, which was due to be held in Zagreb, |

Croatia, in May 2020. The conference was held virtually due to the COVID-19 pandemic. The 81 full papers presented were carefully reviewed and selected from 375 submissions. The papers are organized into the following topical sections: invited talk; best paper awards; obfuscation and functional encryption; symmetric cryptanalysis; randomness extraction; symmetric cryptography I; secret sharing; fault-attack security; succinct proofs; generic models; secure computation I; quantum I; foundations; isogeny-based cryptography; lattice-based cryptography; symmetric cryptography II; secure computation II; asymmetric cryptanalysis; verifiable delay functions; signatures; attribute-based encryption; side-channel security; non-interactive zero-knowledge; public-key encryption; zero-knowledge; quantum II.